CYBERGYM Security Operations Centre (SOC) as a Service

CYBERGYM expertise, applied to testing your technology, policies and people

At CYBERGYM, your cybersecurity is very much our business. To complement our comprehensive range of live cyber training and true-to-life qualification and certification solutions, we also offer a selection of value-added services, including SOC-as-a-Service. Now you can leave it to our experts to identify, mitigate and collect forensics for any cyber incident, while minimizing escalation and brand damage.

SOC as a Service – using CYBERGYM's worldwide experts to monitor and secure your organization

Every day cyberattacks are growing in frequency and severity; organizations, governments and providers of critical services recognize that it's no longer enough for them to rely on technology and internal teams alone. Many are implementing a dedicated, in-house Security Operations Centre (SOC), hiring skilled security personnel to carry out real-time analysis of security data from different systems, and provide a holistic view of the organization's security status detecting suspicious activities, unauthorized access, abnormal behaviour or patterns, and potential attacks.

But establishing a SOC presents its challenges, including the scarcity of professional personnel with proven experience, expertise and knowledge; the cost and time required for initial and ongoing staff training; designing effective data collection and correlation methodologies; and the lead time required until the SOC is up and running. CYBERGYM's SOC-as-a-Service solution offers a cost-effective, reliable alternative to building your own SOC.

How we do it

Our comprehensive SOC-as-a-Service solution gives you the benefits of quick implementation and operation of a SOC, operated and managed 24/7/365 by CYBERGYM's expert team.

- Designing, with you, the data collection methodologies to be implemented, including the systems that will be monitored, the events that will be sent and routine operations (such as updates etc.), and implementing the necessary technology tools
- Designing, with you, the cyber threat model according to which the SIEM system optimization will be determined, and implementing the required SIEM configuration
- Monitoring, detecting and analyzing your organization's security events, in real time
- Safely managing data collected from your organization, including encrypting and sending it to CYBERGYM's SIEM system, where there is a log correlation among various security systems
- Continuously adapting the data collection methodology and system configuration
- Providing access to in-depth reports and dashboards, allowing you to keep your board members and executives informed

SOC-as-a-Service levels

CYBERGYM offers three levels of SOC-as-a-Service:

SOC-as-a-Service Essentials	SOC-as-a-Service Gold	SOC-as-a-Service Platinum
24x7 monitoring.	Ongoing optimization of the SIEM system to your evolving cyber threat model	2-way exchange of security and threat information between your environment and thousands of other sites around the world
Collector software installed in your own environment.	24x7 monitoring	24x7 monitoring
5 admin accounts.	Business hours access to access to CYBERGYM security team for incident investigation	Business hours access to a dedicated CYBERGYM security engineer
Minimum of 8 collectors	Collector software installed in your environment	Collector software installed in your environment
	10 Admin accounts	10 admin accounts
	Access to CYBERGYM's additional services at a discounted rate	Annual Vulnerability Assessment of your IT environment
	Minimum of 10 collectors	Access to CYBERGYM's additional services at a discounted rate
		Minimum of 12 collectors